

## TABLE OF CONTENTS

[Back to AAMI Store](#)

### AAMI Publications

ANSI/AAMI/IEC TIR80001-2-2:2012, <i>Application of risk management for IT networks incorporating medical devices—Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls</i>	p. 4–52
AAMI/IEC TIR80001-2-8:2016, <i>Application of risk management for IT networks incorporating medical devices—Part 2-8: Application guidance— Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2</i>	p. 53–110
AAMI TIR57:2016/(R)2019, <i>Principles for medical device security—Risk management</i>	p. 111–194
TIR97:2018, <i>Principles for medical device security— Postmarket risk management for device manufacturers</i>	p. 195–250
<i>Medical Device Cybersecurity: A Guide for HTM Professionals</i>	p. 251–508
<i>The Medical Device Connectivity FAQs</i>	p. 509–567

### AAMI Resources

A Life Cycle Approach to Medical Device Cybersecurity, Stern G., <i>Biomedical Instrumentation &amp; Technology</i> , November/December 2018, p. 464-466.	p. 568–570
Balancing Patient Safety, Clinical Efficacy, and Cybersecurity with Clinician Partners, Schneider J., Wirth A. <i>Biomedical Instrumentation &amp; Technology</i> , 2021.	p. 571–578
COVID-19 and What It Means for Cybersecurity, Wirth A. <i>Biomedical Instrumentation &amp; Technology</i> , May/June 2020, p. 216-219.	p. 579–582
Finding a Universal Language to Discuss Healthcare Cybersecurity, Roundtable Discussion, <i>Biomedical Instrumentation &amp; Technology</i> , March/April 2020, p. 125-132.	p. 583–590
The Case for Medical Device Cybersecurity Hygiene Practices for Frontline Personnel, Grimes S., Wirth A., <i>Biomedical Instrumentation &amp; Technology</i> , 2021.	p. 591–594
The Evolving State of Medical Device Cybersecurity, Schwartz S., et al. <i>Biomedical Instrumentation &amp; Technology</i> , March/April 2018, p. 103-111.	p. 595–603

## Other Resources

- Best Practices for Communicating Cybersecurity Vulnerabilities to Patients, Center for Devices and Radiological Health*, U.S. Food and Drug Administration, October 2021. p. 604–623
- FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework*, U.S. Food and Drug Administration and The Office of the National Coordinator for Health Information Technology, 2014. p. 624–657
- Framework for improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute of Standards and Technology, April 16, 2018. p. 658–712
- Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff*, U.S. Food and Drug Administration, December 28, 2016 p. 713–742
- Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities*, Discussion Paper, U.S. Food and Drug Administration, June 2021. p. 743–748

[Back to AAMI Store](#)

